ⵛ

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/710,307	07/01/2004	David S. Bonalle	70655.1300	4306

20322   7590   10/10/2006

SNELL & WILMER
400 EAST VAN BUREN
ONE ARIZONA CENTER
PHOENIX, AZ 85004-2202

EXAMINER
WALSH, DANIEL I

ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 10/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

		Application No.	Applicant(s)
Office Action Summary		10/710,307	BONALLE ET AL.
		Examiner	**Art Unit**
		Daniel I. Walsh	2876

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 July 2006.*

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle,* 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____ .

DETAILED ACTION

1.   Receipt is acknowledged of the Amendment received on 7-28-06.

Double Patenting

2.   Claims 1 and 3 are provisionally rejected on the ground of nonstatutory obviousness-type

double patenting as being unpatentable over claims 1 and 20 of copending Application No.

10/710,332.

Although the conflicting claims are not identical, they are not patentably distinct from

each other because they are obvious variants and have the same scope.

For example claims 1 and 3 of the current Application claim "...smartcard...integrated

circuit device...common file structure...partner file structure..." (re claim 1) and "...room key."

(re claim 3), whereas in the '332 Patent Application the Applicants claim

"...smartcards...integrated circuit device...common file structure...partner file structure..." (re

claim 1) and "...room key." (re claim 20).

This is a <u>provisional</u> obviousness-type double patenting rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

4.   Claims 1-13, 15, 17-19, and 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black (US 2005/0122209) in view of Hohle et al. (US 6,101,477).

Re claim 1, Black (US 2005/0122209) teaches a smartcard transaction system configured with a biometric security device, the system comprising: a smartcard configured to communicate with a reader, wherein the reader and biometric security device communicate with a host; a biometric security device comprising a biometric sensor configured to detect a proffered biometric sample, the biometric sample configured to communicate with the system; and, a means to verify the proffered biometric sample to facilitate a transaction (FIG. 1C, which teaches a smartcard (abstract), smartcard reader, biometric sensor (step 6 of FIG. 1C), and steps 7+ which teach authentication and to facilitate a transaction (by a device)). Though Black is silent to a specific verification device, the Examiner notes that it would have been obvious to one of ordinary skill in the art to use a verification device to verify that the sample is an authentic biometric sample, for increased security. The Examiner notes that such devices are conventional in the art and therefore are obvious expedients.

Black is silent to the details of the applications and file structures as claimed.

Hohle et al. teaches such limitations (see claim 1).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black with those of Hohle et al.

One would have been motivated to do this for convenience (applications for user).

It would have been obvious to verify the transaction using the file structure as claimed, as taught by Hohle et al., because the structure stores the relevant information.

Re claim 2, Black teaches the sensor is configured to communicate with the system via at least one of a smartcard, a reader, and a network (FIG. 1C).

Re claims 3 and 16, Hohle et al. teaches a room key and user preferences as claimed (FIG. 4).

Re claim 4, Black teaches that the digital and electronic signatures are captured and preserved in a transaction record (paragraph [0125]). This is interpreted to include logging at least one of a detected biometric sample, processed biometric sample, and stored biometric sample. Though Black is silent to the biometric sensor doing the logging, the Examiner notes that it would have been obvious for the sensor to do the logging, since it captures/receives the inputs. Additionally, though silent to security procedures when the data doesn't match, the Examiner notes that it is well known and conventional to allow users a couple attempts to access a system before performing a security procedure (3 attempts at a password, PIN, etc. before blocking access for a predetermined time). It would have been obvious to allow the user a couple attempts before blocking the user, transponder, etc. to provide the user an attempt to rectify a mistake made during providing biometric information. Such means are well known and conventional in the art for access control, and employing them in a biometric system is an

obvious expedient to provide security, while also allowing a user more than one attempt at access in case a mistake is made.

Re claim 5, Black teaches that a data packet is stored remotely (host computer) where the data packet includes at least one of proffered and registered biometric samples proffered and registered user information, terrorist information, and criminal information (paragraph [0125], FIG. 10A-11B and 14A-14B). The Examiner notes that though such data packet/information is shown with reference to a transponder/RFID, Black states that the device can be a smartcard, transponder, etc. (abstract). Accordingly, it is obvious that such teachings can be applied to smartcards to produce expected results for data storage and retrieval for verifying a transaction using biometrics, especially since it has been taught that such information can be stored on the transponder/card itself or remotely (for security reasons) (paragraph [0090]+). Though silent to a database, the Examiner notes that storing records on a computer in a database is an obvious expedient, well within the skill in the art to organize data for efficient comparison and retrieval.

Re claim 6, as discussed above, the data packet information can be stored on a host computer, which is interpreted to include at least one of the smart card, smartcard reader, sensor, remote server, merchant server, and smartcard system. Though not specifically identified as a server, it would be obvious that the computer is a server, in order to process data/access remotely, for example.

Re claim 7, Black teaches the host computer is associated with the registering and storing/processing of the biometric data used to verify transactions. Though silent to an authorized sample receiver, it is obvious that such a receiver would be authorized, as it is used to facilitate and verify biometrics for transactions.

Re claim 8, Black teaches a device configured to compare a proffered biometric sample with a stored biometric sample (FIG. 1C).

Re claim 9, Black teaches a device configured to compare at least one characteristic of a biometric sample including at least one of minutia, vascular patterns, prints, waveforms, odorants, nodal points, reference points, size, shape, thermal patterns, blood flow, and body heat (FIG. 1C which teaches comparison of fingerprint and signature).

Re claim 10, Black teaches (FIG. 1A) that the host computer can store the reference data. The Examiner notes it would have been obvious for the samples to be stores in a third-party biometric security vendor or government agency as a means to provide secure storage. As the system of Black can be used for point of sale transactions, for example, it would have been obvious that the host computer would be remote from the transaction. Such secure storing of the samples would have been an obvious expedient to protect data and provide security. It is understood that a third party security vendor or government agency can provide such security, and therefore is an obvious expedient for the data storage.

Re claim 11, Black teaches the comparison of sensed data with reference data (FIG. 1C). The reference data is a registered biometric sample.

Re claim 12, Black teaches a registered biometric sample is associated with at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union account information, electronic bill payment information, automatic bill payment information and loyalty point information (abstract, as an account is linked with the biometrics provided during a registration).

Re claim 13, as Black teaches different people using the system with different biometrics, it is obvious that each different sample would be associated with a different account, because different peoples samples would be unique, and each person could have a sample linked to an account.

Re claim 15, as Black teaches that an account is only accessed after a sample is verified, it is interpreted as beginning authentication after the sample is verified.

Re claim 17, though Black is silent to the sensor providing notification upon detection of a sample, the Examiner notes that it is well within the skill in the art to provide notification that a sample has been detected/received (see previous Office Actions reference to Janiak et al.). Though Black is silent to providing notification that a primary account is being accessed, the Examiner notes that the failure to detect a sample/fail to verify a sample, would be evident to the user by a lack of response or a rejected attempt. Positive notification is merely an equivalent. Further, the Applicant has not shown that positive notification of sample detecting would materially affect the workings of the invention, as compared with what can be considered passive notification. The Examiner notes that merely providing notification that the account is being accessed (to the customer/store employee for example) is well known and conventional in the art as evidenced through conventional debit/credit card transactions which indicate to users/workers that authorization is occurring, and through processing and completion of the transaction, positive notification is provided (such as through text, audio, visual, or mere completion of the transaction). It would have been obvious to one of ordinary skill in the art to provide such information, in order to keep the customer/worker aware of the status of the transaction.

Re claim 18, Black teaches the device configured to verify is further configured to facilitate at least one of access, activation of a device, a financial transaction, and a non-financial transaction (abstract, and as the system as a whole facilitates such means, and as a verification device is part of the system is therefore facilitates such means).

Re claim 19, as it has been discussed above re Baer that transactions above a certain amount require a certain biometric, the Examiner has interpreted such teachings as overriding a rule as claimed. As such, as the transactions are conventionally logged, it would have been obvious to report all transactions, including those over a certain amount (requiring a biometric) to the host for record keeping.

Re claim 20, the Examiner notes that preset transaction limitations are known to be associated with a card, and therefore associated by extension to the biometric, such as a maximum credit line/credit purchase, as is conventional in the art for security.

5.   Claim 14 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Hohle et al., as discussed above, in view of de Sylva.

Re claim 14 the teachings of Black/Hohle et al. have been discussed above.

Black/Hohle et al. is silent to the sample being primarily associated with a first user account and secondarily associated with another account, different from the first.

De Sylva teaches such limitations through the use account record 30.

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Hohle et al. with those of de Sylva.

One would have been motivated to do this to have additional accounts associate with a sample for more flexibility and customization for the user.

Re claim 19, Black teaches the device configured to verify is configured to facilitate the use of at least one secondary security procedure (signature, metrics FIG. 1C). Black teaches the use of a transaction record (paragraph [0125]) but it silent to the record occurring during unauthorized access attempts. However, the Examiner notes it would have been obvious to one or ordinary skill in the art to store such attempts in order to obtain security information regarding usage and attempts to access accounts illegally. Additionally, the Examiner notes that it is understood that if access is blocked due to improper authentication, the host would be area of this because the host is the entity through which authentication occurs, and storing such information would have been obvious for security reasons (detecting fraud attempts, system breaches, etc).

Black is silent to the verification device sending a signal to the host device to notify that an established rules for the transponder is being violated.

De Sylva teaches remote database 32 stores non-authenticated data from the verifier (50) (paragraph [0032]).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Baer with those of de Sylva.

One would have been motivated to do this in order to alert instances of fraud. It would have been obvious for the verification device to complete such steps, as it is responsible for verifying the sample, if the sample is not verified it would be obvious to create notification for fraud.

6.   Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Hohle et al., as discussed above, in view of Moebs et al. (US 2005/0065872).

Re claim 14 the teachings of Black/Hohle et al. have been discussed above.

Black/Hohle et al. is silent to the sample being primarily associated with a first user account and secondarily associated with another account, different from the first.

Moebs et al. teaches such limitations (paragraph [0017]).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Baer with those of Moebs et al.

One would have been motivated to do this to have overdraft protection.

7.   Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Hohle et al., as discussed above, in view of Goodman, as cited in the previous Office Action.

Re claim 16, the teachings of Black/Hohle et al. have been discussed above.

Though it is obvious that if the biometric samples do not match that a transaction is not permitted to be executed, Black/Hohle et al. is silent to the smartcard deactivating upon rejection of the biometric sample.

Goodman et al. teaches Goodman et al. teaches deactivation of a card if a predetermined amount of incorrect PIN attempts are detected (paragraph [0029]).

At the time the invention was made, it would have been obvious to an artisan of ordinary skill in the art to combine the teachings of Black/Hohle et al. with Goodman et al.

One would have been motivated to do this to increase the security of the system by disabling a card after a number of incorrect inputs.

Though Goodman is silent to a biometric input, the Examiner notes that Goodman supplies a teaching for disabling a card when a matching input is not received. As Black teaches not allowing a transaction, when a input is not matched (and other reference cited in the previous

Office Action teach contacting authorities), it would have been obvious to use the teachings of

Goodman to expand the security measures and to disable the card so that unauthorized used does

not occur, when biometric inputs do not match, where biometric inputs are interpreted as an

alternative security measure to PIN inputs, to provide additional security. Biometric samples are

a more secure identifier (as taught by Black) but it would still be obvious to disable the card

when the identifiers do not match, whether it be a PIN or biometric, in order to increase

security/reduce fraud.

8.   Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Hohle et

al., as discussed above, in view of Jensen et al. (US 2005/0165684).

    The teachings of Black/Hohle et al. have been discussed above.

    Black/Hohle et al. are silent to notifying the hose if a rule is violated (to be violated).

    Jensen et al. teaches that a sample is required to violate a transaction rule (paragraph

[0081]).

    At the time the invention was made, it would have been obvious to one of ordinary skill

in the art to combine the teachings of Black/Hohle et al. with those of Jensen et al., for additional

security. The Examiner notes it would have been obvious to notify the host, as the host provides

authentication/authorization for transactions. .

Additional Remarks

9.   The Examiner notes that different levels of security are well know and conventional in

the art. For example, Deo et al. (US 5,721,781) teaches based on transaction amounts, different

information is required in order to provide security/assurance that the user is valid (see Fig. 9),

Rasmussen et al. (US 6,834,795) teaches similar teachings (FIG. 5), and Tetro et al. (US

6,095,413) teaches added security trough use of a separate databases).

The Examiner also notes that different types of biometrics for access are known in the art

(see Mann and Baumann) and that the limitations recited in Hohle et al., especially regarding the

file structure, are very similar to that of the current Application.

Response to Arguments

10.   Applicant's arguments with respect to the claims have been considered but are moot in

view of the new ground(s) of rejection. New art has been cited above.

Conclusion

11.   Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.
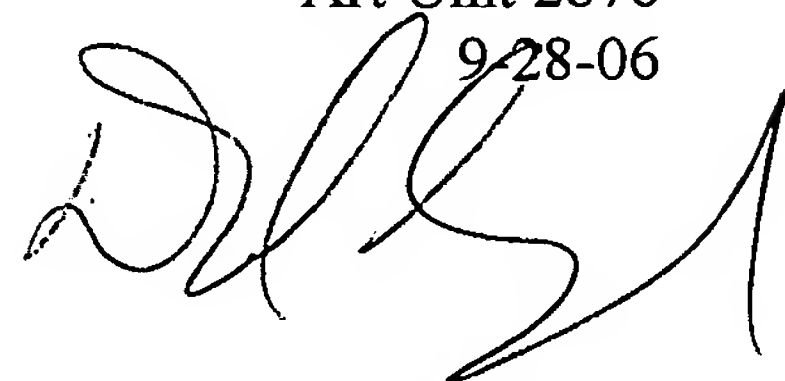
The prior art made of record and not relied upon is considered pertinent to applicant's disclosure (see attached PTO-892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel I. Walsh whose telephone number is (571) 272-2409. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on (571) 272-2398. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Daniel I Walsh
Examiner
Art Unit 2876
9-28-06

**DANIEL WALSH
PRIMARY EXAMINER**